

REMARKS

The Office Action dated April 7, 2009 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 6, and 10-17 have been amended to more particularly point out and distinctly claim the subject matter of the invention. New claims 19-22 have been added. No new matter has been added and a Request for Continued Examination has been concurrently filed along with this response. Therefore, claims 1 and 3-22 are currently pending in the application and are respectfully submitted for consideration.

Claim Rejections Under 35 U.S.C. § 103(a)

The Office Action rejected claims 1, 3, 5 (incorrectly labeled 4 in the heading of the Office Action), 6 and 8-18 under 35 U.S.C. § 103(a) as being unpatentable over Balissat et al. (US 2003/0191843 A1) (herein "Balissat") in view of Bahl et al. (US 2003/0069016 A1) ("Bahl"). The Office Action took the position that Balissat discloses all the elements of the claims with the exception of "detecting a change in the first address of the mobile terminal," "in response to the detecting step, sending an update message to the security gateway, wherein the update message includes a new address value of the first address," and "based on the update message, updating the first address associated with the secure tunnel." The Office Action then cited Bahl as allegedly curing

the deficiencies of Balissat. Applicants respectfully submit that said claims recite allowable subject matter for at least the following reasons.

Claim 1, upon which claims 3-5 are dependent, recites a method, which includes establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, where the first network is a public packet network and the second network is a private packet network and the security gateway connects the first network to a second network and the mobile terminal has a second address that identifies the mobile terminal in the second network. The method further includes, in the security gateway, identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network, and detecting a change in the first address of the mobile terminal. The method further includes, in response to the detecting, sending an update message to the security gateway, where the update message includes a new address value of the first address, and where the update message also includes data to be transmitted to the security gateway. The method further includes, based on the update message, updating the first address associated with the secure tunnel.

Claim 6 recites an apparatus, which includes tunnel establishment means for establishing a secure tunnel to a security gateway through a packet network, where the security gateway is configured to connect a first network to a second network, the first network being a public packet network and the second network being a private packet network, the security gateway is in the second network and the mobile terminal has a

first address that depends on its current location in the first network and a second address that identifies the mobile terminal in the second network. The apparatus further includes address update means for sending an update message through said secure tunnel to the security gateway when the first address changes, where the update message includes a new address value of the first address, and where the update message also includes data to be transmitted to the security gateway.

Claim 9 recites an apparatus, which includes tunnel establishment means for establishing a secure tunnel to a mobile terminal located at a first address in a first network, where the security gateway is in a second network and configured to connect the first network to a second network, the first network being a public packet network and the second network being a private packet network, and the mobile terminal has a second address that identifies the mobile terminal in the second network. The apparatus further includes identification means for identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal, and address update means for updating the first address associated with the secure tunnel, the address update means being responsive to a message received from the mobile terminal, the message including a new value of the first address.

Claim 10 recites a system, which includes tunnel establishment means for establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, where the first network is a public packet network and the second network is a private packet network, the security gateway

is configured to connect the first network to a second network, and the mobile terminal has a second address that identifies the mobile terminal in the second network. The system further includes detection means for detecting a change in the first address, and first address update means, responsive to the detection means, for sending an update message to the security gateway, where the update message includes a new address value of the first address, and where the update message also includes data to be transmitted to the security gateway. The system further includes, in the security gateway, second address update means for updating the first address associated with the secure tunnel in response to the update message, and, in the security gateway, identification means for identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal.

Claim 11 recites a computer useable storage medium having computer readable program code embodied therein to enable a mobile terminal to communicate with a security gateway in a packet-based communication system. The computer readable program code includes computer readable program code configured to cause the mobile terminal to establish a secure tunnel to a security gateway through a packet network, where the security gateway is configured to connect a first network to a second network, the first network being a public packet network and the second network being a private packet network, the security gateway is in the second network and the mobile terminal has a first address that depends on its current location in the first network and a second address that identifies the mobile terminal in the second network. The computer readable

code includes computer readable program code configured to cause the mobile terminal to send an update message through said secure tunnel to the security gateway when the first address changes, where the update message includes a new address value of the first address, and where the update message also includes data to be transmitted to the security gateway.

Claim 12 recites a computer useable medium having computer readable program code embodied therein to enable a mobile terminal located at a first address in a first network to communicate with a security gateway in a packet-based communication system, the security gateway being in a second network and configured to connect a first network to a second network, the first network being a public packet network and the second network being a private packet network. The computer readable program code includes computer readable program code configured to cause the mobile terminal to send an update message through a secure tunnel to the security gateway when a first address that depends on the mobile terminal's current location in the first network changes, where the update message includes a new address value of the first address, and where the update message also includes data to be transmitted to the security gateway.

Claim 13, upon which claims 19-21 are dependent, recites a method, which includes establishing a secure tunnel from a first network to a security gateway in a second network through a packet network, where the security gateway is configured to connect a first network to a second network, the first network is a public packet network and the second network is a private packet network, and the mobile terminal has a first

address that depends on its current location in the first network and a second address that identifies the mobile terminal in the second network. The method further includes sending an update message through said secure tunnel to the security gateway when the first address changes, where the update message includes a new address value of the first address, and where the update message also includes data to be transmitted to the security gateway.

Claim 14, upon which claim 22 is dependent, recites a method, which includes establishing a secure tunnel from a second network to a mobile terminal located at a first address in a first network, where the security gateway is configured to connect the first network to a second network, the first network is a public packet network and the second network is a private packet network, and the mobile terminal has a second address that identifies the mobile terminal in the second network. The method further includes identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal, and updating the first address associated with the secure tunnel in response to a message received from the mobile terminal, the message including a new value of the first address.

Claim 15, upon which claims 7-8 are dependent, recites an apparatus, which includes a control unit, and a memory unit including computer program code. The memory unit and the computer program code are configured to, with the control unit, cause the apparatus at least to, establish a secure tunnel from a first network to a security gateway in a second network through a packet network, where the security gateway is

configured to connect a first network to a second network, the first network is a public packet network and the second network is a private packet network, and the mobile terminal has a first address that depends on its current location in the first network and a second address that identifies the mobile terminal in the second network. The memory unit and the computer program code are also configured to, with the control unit, cause the apparatus at least to send an update message through said secure tunnel to the security gateway when the first address changes, wherein the update message includes a new address value of the first address, and wherein the update message also includes data to be transmitted to the security gateway.

Claim 16, upon which claims 17-18 are dependent, recites an apparatus, which includes a control unit, and a memory unit including computer program code. The memory unit and the computer program code are configured to, with the control unit, cause the apparatus at least to, establish a secure tunnel from a second network to a mobile terminal located at a first address in a first network, where the apparatus is configured to connect the first network to a second network, the first network is a public packet network and the second network is a private packet network and the mobile terminal has a second address that identifies the mobile terminal in the second network. The memory unit and the computer program code are configured to, with the control unit, cause the apparatus at least to, identify the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal, and

update the first address associated with the secure tunnel, being responsive to a message received from the mobile terminal, the message including a new value of the first address.

As will be discussed below, the combination of Balissat and Bahl fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above.

Balissat describes a method and system for providing secure network connections. When a device resides on a private network such that its address is not commonly available to other devices via a public network, a gateway, firewall, or similar device is used to preserve the address of the private network device in confidence while still allowing a secure, end-to-end, connection between the public and private network devices. The gateway or similar devices negotiates separate secure connections with each of the public and private network devices. (See Balissat at Abstract).

Bahl describes a system and method for mobility support which handles address changes of a mobile host. When the mobile host changes to a new address, the mobile host sends an address change message to each of its correspondent hosts over a control channel. Upon receiving the notification, the correspondent host returns an acknowledgment through the control channel and notifies its security filters and transport control parameters corresponding to the connection with the mobile host to use the new address. After receiving the acknowledgment, the mobile host modifies its security filters and transport control parameters for the connection to use the new address. (See Bahl at Abstract).

Applicants respectfully submit that Balissat and Bahl, whether considered individually or in combination, fail to disclose, teach, or suggest, all of the elements of the present claims. For example, the combination of Balissat and Bahl fails to disclose, teach, or suggest, at least, *“identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network,”* as recited in independent claim 1, and similarly recited in independent claims 9, 10, 14, and 16; and *“wherein the update message also includes data to be transmitted to the security gateway,”* as recited in independent claim 1, and similarly recited in independent claims 6, 10-13, and 15.

Regarding *“identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network,”* as recited in independent claim 1, and similarly recited in independent claims 9, 10, 14, and 16, Balissat describes establishing a tunnel between a device 100 and a device 140 via a Gateway 110, where device 140 operates on a private network 130 behind the Gateway 110 and communicates via WAN 120 with device 100. (See Balissat at paragraphs 0045-0048; Figures 1A and 1B).

Furthermore, Balissat describes sending a packet 530 from device 140 through Gateway 110 to device 100. The packet 530 includes a source address B indicating origination at device 140, and a destination address G2, indicating a destination of Gateway 110. As packet 530 is relayed through Gateway 110, the source address is switched to G1, indicating a source of Gateway 110, and the destination address is

switched to A, indicating a destination of device 100. (See Balissat at paragraphs 0085; Figure 5C). However, Balissat further describes that it is possible to share a single G2 address (i.e. Gateway 110 address) between several devices located on private network 130, and in the case of multiple tunnels, a director is used to identify, based on the source address, which IPSec peer corresponds to the flow. (See Balissat at paragraph 0086).

In contrast, independent claim 1 recites “*identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network.*” The claim further defines what is meant by second address, reciting that the second address is an “*address that identifies the mobile terminal in the second network.*” Independent claims 9, 10, 14, and 16 recite similar limitations. Thus, in an embodiment of the invention, a secure tunnel is identified by the address of the mobile terminal that is seen by the terminal in the second network. (See Specification at page 6, line 29 – page 7, line 4). However, Balissat fails to disclose, or suggest, that the tunnel described in Balissat is identified by an address that identifies terminal 100 in the private network 130. Instead, Balissat states that the tunnel is identified on the source address (i.e. the address of terminal 140).

Furthermore, Bahl fails to cure the deficiencies of Balissat. Bahl merely describes sending an address change notification message when a mobile host changes to a new address and sending an acknowledgement message back to the mobile host. (See Bahl at paragraphs 0022-0026; Figure 2). However, Bahl fails to disclose, or suggest, identifying a secure tunnel based on a second address.

Regarding “*wherein the update message also includes data to be transmitted to the security gateway,*” as recited in independent claim 1, and similarly recited in independent claims 6, 10-13, and 15, as the Office Action correctly concludes, Balissat fails to disclose, or suggest, sending an update message. Thus, Balissat clearly fails to disclose, or suggest, an update message which includes data to be transmitted to the security gateway. Accordingly, Balissat fails to disclose, or suggest, the aforementioned limitation.

Furthermore, Bahl does not cure the deficiencies of Balissat. As described above, Bahl discloses that a mobility service 100 of a mobile host sends an address change notification message 102 through a tunnel to a correspondent host 72 when a mobile host changes to a new address. (See Bahl at paragraphs 0022 and 0024). However, the disclosure of Bahl makes clear that the address change notification message 102 (i.e. the control channel message) does not include data to be transmitted. Specifically, Bahl states that the system may send data packets in parallel with control channel message, since the application sending the data is oblivious to the address change and the tunnel migration process. (See Bahl at paragraph 0030). Thus, Bahl makes clear that the control channel message (i.e. address change notification message) is separate and distinct from a data packet, and thus, the control channel message does not include any data to be transmitted via the tunnel. Therefore, Bahl fails to disclose, or suggest, “*wherein the update message also includes data to be transmitted to the security*

gateway,” as recited in independent claim 1, and similarly recited in independent claims 6, 10-13, and 15.

Therefore, for at least the reasons discussed above, the combination of Bahl and Balissat fails to disclose, teach, or suggest, all of the elements of independent claims independent claims 1, 6, 9, and 10-16. For the reasons stated above, Applicants respectfully request that this rejection be withdrawn.

Claims 3 and 5 depend upon independent claim 1. Claim 8 depends upon independent claim 15. Claims 17-18 depend upon independent claim 16. Thus, Applicants respectfully submit that claims 3-4, 15, and 17-18 should be allowed for at least their dependence upon independent claims 1 and 15-16, and for the specific elements recited therein.

The Office Action rejected claims 4 and 7 under 35 U.S.C. § 103(a) as being unpatentable over Balissat in view of Bahl and in further view of Elgebaly et al. (US 2002/0152325 A1). The Office Action took the position that the combination of Balissat and Bahl discloses all the elements of the claims with the exception of “creating a dummy packet.” The Office Action then cited Elgebaly as allegedly curing the deficiencies of Balissat and Bahl. Applicants respectfully submit that said claims recite allowable subject matter for at least the following reasons.

Balissat and Bahl are described above. Elgebaly describes communications protocols operable through network address translation type devices. Specifically, Elgebaly describes communication between a first device having a non-routable address

behind a network address translation type of device (translator), and a second device, according to a protocol in which the first device embeds its non-routable address and a communication port within protocol data sent to the second device. The translator assigns an apparent origin and an apparent port for the protocol data different from the non-routable address and embedded port. The second device is configured to identify the embedded non-routable data and utilize the apparent origin and apparent port. (See Elgebaly at Abstract).

Claim 4 depends upon independent claim 1. Claim 7 depends upon independent claim 15. As discussed above, the combination of Balissat and Bahl does not disclose, teach, or suggest all of the elements of independent claims 1 and 15. Furthermore, Elgebaly does not cure the deficiencies in Balissat and Bahl, as Elgebaly also does not disclose, teach, or suggest, at least, *“identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network,”* as recited in independent claim 1; and *“wherein the update message also includes data to be transmitted to the security gateway,”* as recited in independent claim 1, and similarly recited in independent claim 15. Thus, the combination of Balissat, Bahl, and Elgebaly does not disclose, teach, or suggest all of the elements of claims 4 and 7. Additionally, claims 4 and 7 should be allowed for at least their dependence upon independent claims 1 and 15, and for the specific elements recited therein.

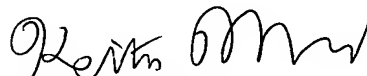
For at least the reasons discussed above, Applicants respectfully submit that the cited prior art references fail to disclose or suggest all of the elements of the claimed

invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1 and 3-22 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Keith M. Mullervy
Registration No. 62,382

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

KMM:sew

Enclosures: Request for Continued Examination Transmittal
Additional Claim Fee Transmittal
Check No. 21046